Remarks

Entry of this amendment, reconsideration of the application, and allowance of all claims are respectfully requested. Upon entrance of this amendment, claims 1, 2, 4, 5, 7-11, 13, 14, 16, 17, 19, 21-29, 31, 32 & 34-38 will remain pending.

Applicants gratefully acknowledge the Board's reversal of the previously-stated 35 U.S.C. §103(a) rejection to the prior pending claims, and acknowledge the new ground of rejection stated by the Board under the first paragraph of 35 U.S.C. §112 for lack of written description and lack of enablement. Although Applicants believe that the specification as filed inherently provided support for simultaneously changing multiple encryption parameters, the word "simultaneously" does not expressly appear in the application as filed. Therefore, in order to further prosecution of the subject application, Applicants are herein deleting the word "simultaneously" from the pending claims. Based upon this amendment, withdrawal of the 35 U.S.C. §112 rejection is requested.

By this paper, independent claims 1, 14, 27 & 28 are further amended to recite the subject matter of canceled dependent claims 12 & 18. More particularly, Applicants' independent claims now recite the dynamic varying of the encrypting of the stream of data at the encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data. Support for this amended language can be found in the canceled dependent claims 12 & 18, as well as the specification as filed. For example, reference page 7, lines 22-25. Thus, no new matter is added to the application by any amendment presented.

In view of the cancellation of the word "simultaneously", and the addition of the further characterization of dynamically varying encryption of the stream of data at the encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data, Applicants herein address the previously-applied art of record with respect to the now-presented language. Specifically, Applicants respectfully submit that the amended independent claims presented herewith patentably distinguish over Jones (U.S. Patent No. 5,412,730; hereinafter "Jones"), Nardone et al. (U.S. Patent No. 5,805,700; hereinafter "Nardone"), and Leppek (U.S. Patent No. 5,933,501; hereinafter "Leppek").

EN998146

- 10 -

As recited in claim 1, for example, applicants' invention comprises a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The method includes encrypting the stream of data at the encryption unit for transferring of the encrypted stream of data from the encryption unit to the decryption unit. The encrypting of the stream of data is dynamically varied at the encryption unit over multiple portions of the stream of data by dynamically changing multiple encryption parameters of the encryption process employed for each portion of the stream of data, and signaling the dynamic change in encryption parameters to the decryption unit. The dynamically varying of the multiple encryption parameters is responsive to occurrence of a predefined condition in the stream of data. Upon receipt of the encrypted data at the decryption unit, the method includes decrypting the encrypted data, wherein the decrypting accounts for the dynamic varying of the encrypting by the encryption unit using the changed, multiple encryption parameters.

Advantageously, the present invention provides a new technique for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The technique includes dynamically <u>changing multiple encryption parameters over multiple portions of the stream of data</u> used to encrypt each portion of the stream of data <u>as the stream of data is passing through the encryption unit</u>. This dynamically changing can occur periodically over time, for example, several times a second, thereby allowing only a small portion of the stream of data to be decoded should the encryption parameters used to encrypt that portion of data be uncovered. This concept of dynamically changing multiple encryption parameters as a stream of data is being encrypted is believed to comprise a unique approach from any of the applied art, which typically rely upon definition of a predefined policy for changing the encryption process.

Jones describes an encrypted data transmission system employing means for "randomly" altering the encryption keys. Pseudo-random number generators are employed at both the transmitting and receiving stations to supply identical sequences of encryption keys to a transmitting encoder and receiving decoder. An initial random number seed value is made available to both stations. The random number generators are advanced at times determined by predetermined characteristics of the data being transmitted so that, after transmission has taken place, the common encryption key can be known only to the transmitting and receiving stations.

EN998146

- 11 -

A careful reading of Jones fails to uncover any teaching or suggestion of applicants' concept of encrypting a stream of data and during the encryption process dynamically varying encrypting of the stream of data over multiple portions of the stream of data by dynamically changing multiple encryption parameters employed for each portion of the stream of data. The Jones encryption approach requires pseudo-random binary sequence generation, and requires seed and mask values arranged at the sender and the receiver. Further, a change in Jones to the encryption process involves changing only an encryption key. The change in the encryption key occurs only at a predefined interval arranged a priori between the sender and the receiver. Jones changes the encryption key only when the counted number of bits or words or "items" matches the arranged interval. The disadvantage of this approach is that synchronization is absolutely essential. Bytes lost during transmission throw off the encryption/decryption process without any chance of recovery. In contrast, applicants' invention of dynamically varying multiple encryption parameters employed for each portion of the stream of data as the stream of data is being encrypted ensures that only a small portion of the encrypted data could be exposed or lost should the encryption parameters used to encrypt that segment become uncovered or lost, respectively.

In addition, applicants' recited process includes signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit. A careful reading of Jones fails to uncover any teaching, suggestion or implication that the single encryption key change is signaled to the decryption unit. Rather, the patent teaches otherwise by describing a process which relies upon an a priori agreed upon process. In Jones, the decryption unit knows in advance where the encryption key change is to occur. In contrast, applicants recite a truly dynamic varying of the encryption process wherein the dynamically changed encryption keys are forwarded from the encryption unit to the decryption unit.

At page 35 of the prior final Office Action, the Examiner states that Applicants' recited aspect of "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit" is taught by Jones at Col. 1, lines 66 to Col. 2, line 7, wherein there is an alleged exchange of random number seed values and interval values between the encryptor and decryptor. Applicants respectfully submit that these lines of Jones disclose an a priori

arrangement whereby the seed values and interval values are made available to both the transmitting station and a receiving station. Fig. 1 of Jones clearly shows that the interval number and random number seed are inputs to both stations. The transmitting station does not forward the interval number and seed number to the receiving station. Thus, there is no dynamic signaling of encryption information *per se* from the encryption unit to the decryption unit in Jones.

Nardone describes a policy based selective encryption of compressed video data. Basic transfer units of compressed video data of a video image are selectively encrypted in Nardone in accordance with an encryption policy to degrade the video image to at least a virtually useless state, i.e., if the selectively encrypted compressed video image were to be rendered without decryption. A careful reading of Nardone fails to uncover any dynamic varying of the encryption parameters as a stream of data is being encrypted within an encryption unit as recited by applicants. The prior final Office Action notes that Nardone teaches encrypting of a bit stream taking into account encryption granularity, density and delay. However, Nardone does not describe dynamically varying multiple ones of these encryption parameters as the encryption of a stream of data progresses.

Nardone is characterized in the final Office Action as teaching specifying encryption parameters via a policy (i.e., the degree of selective encryption in order to degrade video image). This characterization of the teachings of Nardone is traversed. Nardone does not expressly describe varying of multiple encryption parameters, let alone varying multiple encryption parameters dynamically for multiple portions of the stream of data during the encryption process. Nardone does teach multiple encryption polices can be provided at authoring time, and does discuss the possibility of changing between policies. However, Applicants respectfully submit that this change between policies merely results in a change in the duty cycle of the encryption process in Nardone, and does not depend upon or suggest that multiple encryption parameters are changed between the policies. A careful reading of Nardone fails to uncover any teaching or suggestion of such a concept. Notwithstanding this, the prior final Office Action characterizes the change in encryption policy (resulting in a change in the duty cycle in Nardone) as somehow equating to a dynamic change in multiple encryption parameters during the encryption process. Applicants respectfully submit that a change between predefined policies in Nardone doe not

equate to or suggest their recited process for dynamically varying the encrypting of a stream of data at an encryption unit by dynamically changing multiple encryption parameters between different portions of the stream of data. The result of Nardone is simply a change in the duty cycle of the encryption process, and does not suggest that multiple encryption parameters are varied during the encryption process. Thus, without hindsight reference to Applicants' claimed invention, it is respectfully submitted that one of ordinary skill in the art would not have read the teachings of Nardone as suggesting that multiple encryption parameters could be varied dynamically for multiple portions of the stream of data during the encryption process.

In Nardone, an encryption policy refers to the encryption duty cycle. As stated at column 1, lines 40-59 thereof, Nardone achieves degradation that approximates the level provided by a total encryption approach, but requires only a fraction of the processor cycle cost of the total encryption approach by selectively encrypting certain basic transfer units. This selective encryption occurs in Nardone at authoring time; and at authoring time, which basic transfer units are to be encrypted may be dynamically adjusted. As explained by Nardone, in one embodiment, where the video images are MPEG compressed, all BTUs containing either the start code for a group of pictures or the start code for a particular frame are encrypted, to prevent recovery of the video frames. In an alternate embodiment, a fraction of the BTUs of an I frame, and a fraction of the BTUs of a P frame are encrypted, again, to destroy data references by future frames. Thus, the goal of Nardone is to reduce the processor cycle cost required to entirely encrypt video data of video images. The dynamic adjustment of encryption policies in Nardone is taught to change which basic transfer units are to be encrypted (i.e., the duty cycle of the encryption process), and not the encryption process *per se*. This change in the amount of encryption being applied to the video data of the video images does not teach or suggest that multiple encryption parameters are changed over multiple portions of a stream of data.

To summarize, Nardone describes a change in encryption policies to effect the amount of partial encryption applied to video data of a video image in order to ensure sufficient degradation of the video image to a virtually useless state (i.e., if the selectively encrypted compressed video images were to be rendered without decryption), while requiring only a fraction of the processor cycle cost compared to a total encryption process. Because the policy selection at authoring time described by Nardone only presents a change in the duty cycle, i.e., a change in which basic

EN998146

transfer units of the video data are to be encrypted, Applicants respectfully submit that Nardone does not provide an insight as characterized by the Examiner in previous papers. The only "parameter" being changed with a dynamic adjustment in policy in Nardone is a change in the duty cycle of the encryption of the basic transfer units. There is no teaching or suggestion in Nardone that a change in encryption policy from one fractual encryption to another fractual encryption equates to a change in multiple encryption parameters between different portions of a stream of data. To characterize the teachings of Nardone otherwise is believed to result from a hindsight reference to Applicants' own invention.

Leppek describes a virtual encryption scheme which combines different encryption operators into a compound-encryption mechanism. The encryption operators in Leppek refer to different encryption processes. Thus, in Leppek, data is first encoded using a first encryption scheme, then the same data is encoded using a second encryption scheme, etc., thereby increasing the entropy of the data to make the encoded data look as random as possible.

In contrast, applicants recite dynamically changing multiple encryption parameters employed for each portion of a stream of data while an encryption unit is encrypting a stream of data. In applicants' approach, different segments of a stream of data are encrypted using different encryption parameters and there is a dynamic change in the encryption parameters such that multiple encryption parameters change from one segment to another segment of the stream of data as the stream of data is passing through the encryption unit and being encrypted. In Leppek, there is a static, sequential application of a number of encryption algorithms or encryption operators to the same segment of data. Leppek describes encrypting the same data multiple times using different encryption operators (i.e., encryption schemes).

At page 33 of the final Office Action, the Examiner seeks to equate Leppek's teaching of a compound sequence of encryption operators, i.e., the sequential application of encryption algorithms, to Applicants' recited language of changing multiple encryption parameters employed for each portion of the stream of data during the dynamically varying of the encrypting of the stream of data. The alleged insight of Leppek is application of multiple encryption operators at once. Leppek describes a sequential application of encryption algorithms to the same data to increase the entropy of the data. Since Leppek describes a process of sequentially

applying different encryption processes to the same data, Applicants respectfully submit that the insight allegedly drawn therefrom is in error.

Additionally, to the extent deemed relevant to the claims presented herewith, Applicants respectfully submit that one of ordinary skill in the art would not have combined Jones, Nardone and Leppek as proposed in the final Office Action. For example, Jones relies on a fixed policy or fixed sequence for changing a single encryption parameter. Nardone describes a process for varying the duty cycle of an encryption scheme based on predefined policies, and Leppek describes a virtual encryption scheme which combines different encryption processes into a sequential, compound encryption mechanism. None of these references, taken singularly or in combination, suggest Applicants' recited concept of dynamically changing the encryption process over multiple portions of the stream of data by changing multiple encryption parameters employed for each portion of the stream of data as a stream of data is being encrypted. Because Applicants' approach does not rely upon any predefined policy, the dynamic change in the multiple encryption parameter is signaled from the encryption unit to the decryption unit. Jones, Nardone, and Leppek do not describe any mechanism for signaling dynamic changes in multiple parameters from an encryption unit to a decryption unit. In this regard, Jones does not describe signaling of encryption parameter changes from the encryption unit to the decryption unit. In Jones, a seed value and interval value are established a priori before an encryption process begins and are provided as inputs to both the encryption unit and the decryption unit (see Fig. 1 of Jones). Since they are provided a priori as inputs to both units, there is no signaling from the encryption unit to the decryption unit of the simultaneous change of multiple encryption parameters.

For the above reasons, Applicants respectfully request reconsideration and allowance of independent claims 1, 14 & 27. Claims 1 & 14 are also believed allowable over the combination of Aucsmith et al. (U.S. Patent No. 5,991,403), Nardone and Leppek stated in the final Office Action. The teachings of Aucsmith et al. are similar to those of Jones when applied against the independent claims presented, and are believed distinguishable for the reasons stated above in connection with Jones. As noted in the final Office Action, Aucsmith teaches generation of an encryption key for each Group Of Pictures (GOP) in a stream of video data. For each GOP, an encryption transformation, parameterized by the encryption key of the GOP, is applied to
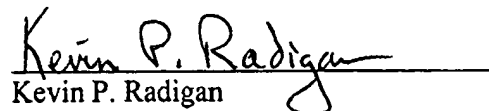
pictures of the GOP. Applicants respectfully submit that Aucsmith teaches an approach for changing a single encryption parameter between GOPs, and is therefore analogous to the teachings of Jones described above when applied against Applicants' independent claims.

Similarly, the rejection to independent claim 28 based upon Warren et al. (U.S. Patent No. 5,719,937) in view of Nardone and Leppek is respectfully traversed for the reasons stated herein above with respect to Jones, Nardone and Leppek. Warren et al. describe an encryption process using a scheme such as Hidden Data Transport (HDT) and Post-Compression Hidden Data Transport (PC-HDT). Warren et al. describe certain advantages of using HDT and PC-HDT algorithms over other encoding technologies, but does not even describe switching between HDT and PC-HDT algorithms dynamically. Thus, Applicants respectfully submit that Warren et al. is less relevant to their claimed invention than the Jones patent described above.

The dependent claims are believed allowable for the same reasons that the independent claims from which they directly or ultimately depend, as well as for their own additional characterizations. Chiariglione '98 is not believed to teach or suggest any of the above-noted deficiencies of Jones, Nardone, Leppek, Aucsmith et al. or Warren et al. when applied against the independent claims presented herewith.

All pending claims are believed to be in condition for allowance and such action is respectfully requested. Should the Examiner wish to discuss this case with Applicants' attorney, the Examiner is invited to contact Applicants' representative at the below-listed number.

Respectfully submitted,

Kevin P. Radigan
Kevin P. Radigan
Attorney for Applicants
Reg. No. 31,789

Dated: August _11_, 2005

HESLIN ROTHENBERG FARLEY & MESITI, P.C.
5 Columbia Circle
Albany, New York 12203
Telephone: (518) 452-5600
Facsimile: (518) 452-5579